**Утвърждавам,**
**КМЕТ:**
**/Николай Мелемов/**

**Дата: 13.01.2022 г.**

## „ДЕКЛАРАЦИЯ ЗА ПРИЛОЖИМОСТ”

| НАИМЕНОВАНИЕ НА КОНТРОЛИТЕ | | | Да / Не | | ВНЕДРЯВАНЕ |
|---|---|---|---|---|---|
| **А.5** | **Политики за сигурност на информацията** | | | | |
| А.5.1 | **Насока за управление на сигурността на информацията** | | | | |
| ***Цел:*** *Да осигури насока за управление и поддържане на сигурността на информацията в съответствие с изискванията за дейността и изискванията на съответното законодателство и нормативни актове.* | | | | | |
| **А.5.1.1** | **Дейност:**<br>Политики по сигурност на информацията | **Контрол:**<br>Трябва да бъде определен набор от политики за сигурност на информацията, одобрен от ръководството, разпространен и разгласен на всички служители и съответните външни страни. | Да<br>√ | Не | |
| **А.5.1.2** | **Дейност:**<br>Преглед на политиките за сигурност на информацията | **Контрол:**<br>Политиките за сигурност на информацията трябва да бъдат подлагани на преглед през планирани интервали или при настъпване на значителни промени, за да се гарантира постоянно тяхната актуалност, адекватност и ефикасност. | Да<br>√ | Не | |
| **А.6** | **Организиране на сигурността на информацията** | | | | |
| **А.6.1** | **Вътрешна организация** | | | | |
| ***Цел:*** *Да установи управленска рамка за въвеждане и контрол на реализирането и оперирането на сигурност на информацията в рамките на организацията.* | | | | | |
| А.6.1.1 | **Дейност:**<br>Роли и отговорности по сигурността на информацията | **Контрол:**<br>Трябва да бъдат определени и разпределени всички отговорности по сигурността на информацията | Да<br>√ | Не | |
| А.6.1.2 | **Дейност:**<br>Разделяне на задълженията | **Контрол:**<br>Трябва да бъдат разделени противоречивите задължения и области на отговорност, за да бъдат намалени възможностите за неоторизирано или неумишлено модифициране, или злоупотреба с активите на организацията. | Да<br>√ | Не | |
| А.6.1.3 | **Дейност:**<br>Контакт с оторизираните органи | **Контрол:**<br>Трябва да се поддържат подходящи контакти със съответните оторизирани органи. | Да<br>√ | Не | |

| | | | | | |
|---|---|---|---|---|---|
| A.6.1.4 | **Дейност:**<br>Контакт с групи със специален интерес | **Контрол**:<br>Трябва да бъдат поддържани подходящи контакти с групи със специален интерес или други форуми на специалисти по сигурността и професионални асоциации. | Да<br>√ | Не | |
| A.6.1.5 | **Дейност:**<br>Сигурност на информацията при управление на проекти | **Контрол:**<br>Независимо от вида на проекта трябва да бъде отчетена сигурността на информацията при управление на проекти. | Да<br>√ | Не | |
| **A.6.2** | **Мобилни устройства и работа от разстояние** | | | | |
| ***Цел:*** *Да осигури сигурност при работа от разстояние и използване на мобилни устройства.* | | | | | |
| A.6.2.1 | **Дейност:**<br>Политика за мобилните устройства | **Контрол:**<br>Трябва да бъдат приети политика и поддържащи мерки за сигурност за управление на рисковете, внесени от използването на мобилни устройства. | Да<br>√ | Не | |
| A.6.2.2 | **Дейност:**<br>Работа от разстояние | **Контрол:**<br>Трябва да бъдат приложени политика и поддържащи мерки за сигурност, за да се защити достъпната, обработваната или съхраняваната информация в местата за работа от разстояние. | Да<br>√ | Не | |
| **A.7** | **Сигурност на човешките ресурси** | | | | |
| **A.7.1** | **Преди наемане на работа** | | | | |
| ***Цел:*** *Да се гарантира, че служители и доставчици разбират своите отговорности и са подходящи за ролите, които ще изпълняват.* | | | | | |
| A.7.1.1 | **Дейност:**<br>Подбор на кадри | **Контрол:**<br>Трябва да бъде извършвано проучване за проверка на биографичните данни на всички кандидати за наемане на работа в съответствие със съответните закони, нормативни актове и етика и съобразно изискванията, свързани с дейността, класификацията на информацията, до която имат достъп, и предполагаемите рискове. | Да<br>√ | Не | |
| A.7.1.2 | **Дейност:**<br>Срокове и условия за наемане на работа | **Контрол:**<br>Договорни споразумения със служителите и доставчиците трябва да определят техните отговорности и отговорностите на организацията по отношение на сигурността на информацията. | Да<br>√ | Не | |
| **A 7.2.** | **По време на работа** | | | | |
| ***Цел:*** *Да се гарантира, че служителите и доставчиците са запознати и изпълняват своите отговорности по отношение на сигурността на информацията.* | | | | | |
| A.7.2.1 | **Дейност:**<br>Отговорности на ръководството | **Контрол:**<br>Ръководството трябва да изисква от служителите и доставчиците да прилагат мерките за сигурност в съответствие с установените политики и процедури на организацията. | Да<br>√ | Не | |
| A.7.2.2 | **Дейност:**<br>Осъзнаване, образование и обучение по сигурност на информацията | **Контрол:**<br>В съответствие със своите работни функции всички служители на организацията и, където е уместно, доставчиците трябва да получат подходящо обучение с цел осъзнаване и редовно актуализиране на знанията по политиките и процедурите на организацията. | Да<br>√ | Не | |

| | | | | | |
|---|---|---|---|---|---|
| A.7.2.3 | **Дейност:**<br>Дисциплинарен процес | **Контрол:**<br>За служители, извършили нарушение по отношение на сигурността на информацията, трябва да има официален и оповестен дисциплинарен процес. | Да<br>√ | Не | |
| **A.7.3** | **Прекратяване или промяна на трудовите отношения** | | | | |
| ***Цел:*** *Да се защитят интересите на организацията като част от процеса за промяна или прекратяване на трудовите правоотношения.* | | | | | |
| A.7.3.1 | **Дейност:**<br>Отговорности при прекратяване или промяна на трудовото отношение | **Контрол:**<br>Отговорностите и задълженията по отношение сигурността на информацията при прекратяване или промяна на трудовото отношение трябва да бъдат определени, оповестени на служителя или доставчика и приведени в действие. | Да<br>√ | Не | |
| **A.8** | **Управление на активи** | | | | |
| **A8.1** | **Отговорност за активите** | | | | |
| ***Цел:*** *Да се идентифицират активите на организацията и да се определят съответните отговорности за защитата им.* | | | | | |
| A.8.1.1 | **Дейност:**<br>Опис на активите | **Контрол:**<br>Всички активи, свързани с информационните средства и средствата за обработване на информация, трябва да бъдат ясно идентифицирани и на тези активи трябва да бъде съставен и поддържан опис. | Да<br>√ | Не | |
| A.8.1.2 | **Дейност:**<br>Притежание на активи | **Контрол:**<br>Активите, поддържани в описа, трябва да бъдат притежавани. | Да<br>√ | Не | |
| A.8.1.3 | **Дейност:**<br>Допустимо използване на активи | **Контрол:**<br>Трябва да бъдат посочени, документирани и прилагани правила за допустимо използване на информация и активи, свързани с информацията и средствата за обработване на информация. | Да<br>√ | Не | |
| A.8.1.4 | **Дейност:**<br>Връщане на активи | **Контрол:**<br>Всички служители и потребители от трета страна при прекратяване на тяхното трудово отношение, договор или споразумение трябва да върнат всички притежавани от тях активи на организацията. | Да<br>√ | Не | |
| **A.8.2** | **Класифициране на информацията** | | | | |
| ***Цел:*** *Да се гарантира, че информацията получава необходимата степен на защита в съответствие с важността ѝ за организацията.* | | | | | |
| A.8.2.1 | **Дейност:**<br>Класифициране на информацията | **Контрол:**<br>Информацията трябва да бъде класифицирана според изискванията на нормативните актове, нейната стойност, критичност и чувствителност към неоторизирано разкриване или модифициране. | Да<br>√ | Не | |
| A.8.2.2 | **Дейност:**<br>Означаване и работа с информация | **Контрол:**<br>Информацията трябва да бъде класифицирана според изискванията на нормативните актове, нейната стойност, критичност и чувствителност към неоторизирано разкриване или модифициране. | Да<br>√ | Не | |
| A.8.2.3 | **Дейност:**<br>Работа с активи | **Контрол:**<br>Трябва да бъдат разработени и приложени процедури за работа с активи в съответствие с класификационната схема на информацията, приета от организацията. | Да<br>√ | Не | |

| | | | | | |
|---|---|---|---|---|---|
| **A.8.3** | **Работа с информационни носители** | | | | |
| ***Цел:*** *Да се предотврати неоторизирано разкриване, изменение, премахване или разрушаване на информация, съхранявана върху носители.* | | | | | |
| A.8.3.1 | **Дейност:**<br>Управление на сменяеми носители | **Контрол:**<br>Трябва да има внедрени процедури за управлението на сменяеми информационни носители в съответствие с класификационната схема, приета от организацията. | Да<br>√ | Не | |
| A.8.3.2 | **Дейност:**<br>Унищожаване на носители | **Контрол:**<br>Ненужните носители трябва да се унищожават по сигурен начин, като се използват официални процедури. | Да<br>√ | Не | |
| A.8.3.3 | **Дейност:**<br>Пренасяне на физически носители | **Контрол:**<br>По време на транспортиране носителите, съдържащи информация, трябва да бъдат защитени срещу неоторизиран достъп, използване не по предназначение или подправяне. | Да<br>√ | Не | |
| **A 9** | **Контрол на достъпа** | | | | |
| **A.9.1** | **Изисквания за дейността за контрол на достъпа** | | | | |
| ***Цел:*** *Да се ограничи достъпът до информацията и средствата за обработване на информация.* | | | | | |
| A.9.1.1 | **Дейност:**<br>Политика за контрол на достъпа | **Контрол:**<br>Трябва да бъде създадена, документирана и подлагана на преглед политика за контрол на достъпа, основана на изискванията за дейността и изискванията за сигурност на информацията. | Да<br>√ | Не | |
| A.9.1.2 | **Дейност:**<br>Достъп до мрежи и мрежови услуги | **Контрол:**<br>На потребителите трябва да бъде осигурен достъп само до тези мрежи и мрежови услуги, за които те са изрично оторизирани да използват. | Да<br>√ | Не | |
| **A.9.2** | **Управление на достъпа на потребителите** | | | | |
| ***Цел:*** *Да се гарантира оторизиран достъп на потребителите и да се предотврати неоторизиран достъп до системи и услуги.* | | | | | |
| A.9.2.1 | **Дейност:**<br>Регистрация и прекратяване на регистрацията на потребители | **Контрол:**<br>Трябва да бъде реализиран официален процес за регистрация и прекратяване на регистрацията на потребителите, който да предостави присвояване на права за достъп | Да<br>√ | Не | |
| A.9.2.2 | **Дейност:**<br>Осигуряване на достъп на потребители | **Контрол:**<br>Трябва да бъде реализиран официален процес за предоставяне на достъп на потребителите, който да предостави или отнеме правата за достъп на всички видове потребители до всички системи и услуги. | Да<br>√ | Не | |
| A.9.2.3 | **Дейност:**<br>Управление на привилегировани права за достъп | **Контрол:**<br>Предоставянето и използването на привилегировани права за достъп трябва да бъде ограничено и контролирано. | Да<br>√ | Не | |
| A.9.2.4 | **Дейност:**<br>Управление на тайната информация за автентификация на потребителите | **Контрол:**<br>Предоставянето на тайна информация за автентификация трябва да бъде контролирано чрез официален процес за управление. | Да<br>√ | Не | |

| | | | | | |
|---|---|---|---|---|---|
| A.9.2.5 | **Дейност:**<br>Преглед на правата за достъп на потребителите | **Контрол:**<br>Собствениците на активи трябва да преглеждат правата за достъп на потребителите през редовни интервали. | Да<br>√ | Не | |
| A.9.2.6 | **Дейност:**<br>Отнемане или коригиране на права за достъп | **Контрол:**<br>Правата за достъп на всички служители или потребители от трета страна до информацията и до средствата за обработване на информация трябва да бъдат отнети при прекратяване на тяхното трудово отношение, договор или споразумение или коригирани при настъпване на промяна. | Да<br>√ | Не | |
| **A 9.3** | **Отговорности на потребителите** | | | | |
| ***Цел:*** *Да се държат потребителите отговорни за защита на тяхната информация за автентификация.* | | | | | |
| **A.9.3.1** | **Дейност:**<br>Използване на тайна информация за автентификация | **Контрол:**<br>Трябва да се изисква от потребителите да следват практиките на организацията при използването на тайна информация за автентификация. | Да<br>√ | Не | |
| **A.9.4** | **Контрол на достъпа до системи и приложения** | | | | |
| ***Цел:*** *Да се предотврати неоторизиран достъп до системи и приложения.* | | | | | |
| A.9.4.1 | **Дейност:**<br>Ограничаване на достъпа до информация | **Контрол:**<br>Трябва да бъде ограничен достъпът до информация и функциите на приложните системи в съответствие с политиката за контрол на достъпа. | Да<br>√ | Не | |
| A.9.4.2 | **Дейност:**<br>Процедури за сигурно влизане в системата | **Контрол:**<br>Когато се изисква от политиката за контрол на достъпа, достъпът до системи и приложения трябва да бъде контролиран чрез процедура за сигурно влизане в системата. | Да<br>√ | Не | |
| A.9.4.3 | **Дейност:**<br>Система за управление на пароли | **Контрол:**<br>Системите за управление на пароли трябва да бъдат интерактивни и да осигуряват качество на паролите. | Да<br>√ | Не | |
| A.9.4.4 | **Дейност:**<br>Използване на привилегировани обслужващи програми | **Контрол:**<br>Използването на обслужващи програми, които биха могли да преодолеят механизмите за контрол на системата и приложенията, трябва да бъде ограничено и строго контролирано. | Да<br>√ | Не | |
| A.9.4.5 | **Дейност:**<br>Контрол на достъпа до изходен код на програмите | **Контрол:**<br>Достъпът до изходния код на програмите трябва да бъде ограничен. | Да<br>√ | Не | |
| **A.10** | **Криптография** | | | | |
| ***Цел:*** *Да се защитят поверителността, достоверността и/или цялостността на информацията чрез правилно и ефикасно използване на криптография.* | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| A.10.1.1 | **Дейност:**<br>Политика за използване на криптографски механизми за контрол | **Контрол:**<br>Трябва да бъде разработена и провеждана политика за използването на криптографски механизми за контрол с цел защита на информацията. | Да<br>√ | Не | |
| A.10.1.2 | **Дейност:**<br>Управление на ключове | **Контрол:**<br>Трябва да се разработи и внедри управление на използването, защитата и времето на живот на криптографските ключове през целия им жизнен цикъл. | Да<br>√ | Не | |
| **A.11** | **Физическа сигурност и сигурност на заобикалящата среда** | | | | |
| **A.11.1** | **Сигурни зони** | | | | |
| ***Цел:*** *Да се предотврати неоторизиран физически достъп, вреда и вмешателство в информацията и средствата за обработване на информация на организацията.* | | | | | |
| A.11.1.1 | **Дейност:**<br>Граници за физическа сигурност | **Контрол**:<br>За защита на зони, които съдържат или чувствителна, или критична информация и средства за обработване на информация, трябва да се определят и използват граници за сигурност. | Да<br>√ | Не | |
| A.11.1.2 | **Дейност:**<br>Механизми за контрол на физическо влизане | **Контрол:**<br>Сигурните зони трябва да бъдат защитени със съответни механизми за контрол на влизане, за да се гарантира, че само оторизираният персонал има разрешен достъп. | Да<br>√ | Не | |
| A.11.1.3 | **Дейност:**<br>Осигуряване на офиси, зали и съоръжения | **Контрол:**<br>Трябва да бъде проектирана и приложена физическа защита за офиси, зали и съоръжения. | Да<br>√ | Не | |
| A.11.1.4 | **Дейност:**<br>Защита от външни заплахи и заплахи от околната среда | **Контрол:**<br>Трябва да бъде проектирана и приложена физическа защита от природни бедствия, злонамерени атаки или инциденти. | Да<br>√ | Не | |
| A.11.1.5 | **Дейност:**<br>Работа в сигурни зони | **Контрол:**<br>Трябва да бъдат разработени и приложени процедури за работа в сигурни зони. | Да<br>√ | Не | |
| A.11.1.6 | **Дейност:**<br>Зони за доставки и зареждане | **Контрол:**<br>Местата за достъп като зони за доставки и зареждане и други места, където неупълномощени лица могат да влязат в помещенията, трябва да бъдат контролирани и ако е възможно, изолирани от средствата за обработване на информация, за да се избегне неоторизиран достъп. | Да<br>√ | Не | |
| **A.11.2** | **Устройства** | | | | |
| ***Цел:*** *Да се предотвратят загуби, повреди, кражби или излагане на риск на активите и прекъсване на дейностите на организацията.* | | | | | |
| A.11.2.1 | **Дейност:**<br>Разполагане и защита на устройствата | **Контрол:**<br>Устройствата трябва да бъдат разположени и защитени, така че да се намалят рисковете от заплахи и опасности от околната среда и възможности за неоторизиран достъп. | Да<br>√ | Не | |
| A.11.2.2 | **Дейност:**<br>Поддържащи комунални системи | **Контрол:**<br>Устройствата трябва да бъдат защитени от повреди в електрозахранването и други разриви, предизвикани от откази в поддържащите комунални системи. | Да<br>√ | Не | |

| | | | | | |
|---|---|---|---|---|---|
| A.11.2.3 | **Дейност:**<br>Сигурност на окабеляването | **Контрол:**<br>Окабеляването за електрозахранване и телекомуникации, носещо данни или поддържащо информационни услуги, трябва да бъде защитено от подслушване, смущения или повреда. | Да<br>√ | Не | |
| A.11.2.4 | **Дейност:**<br>Поддържане на устройствата | **Контрол:**<br>Устройствата трябва да бъдат правилно поддържани, за да се осигури тяхната непрекъсната готовност и цялостност. | Да<br>√ | Не | |
| A.11.2.5 | **Дейност:**<br>Изнасяне на собственост | **Контрол:**<br>Устройства, информация или софтуер не трябва да бъдат изнасяни извън организацията без предварително разрешение. | Да<br>√ | Не | |
| A.11.2.6 | **Дейност:**<br>Сигурност на устройства и активи извън помещенията | **Контрол:**<br>Сигурността трябва да бъде прилагана и към активи, които са извън организацията, като се отчитат различните рискове при работа извън помещенията на организацията. | Да<br>√ | Не | |
| A.11.2.7 | **Дейност:**<br>Сигурно унищожаване или повторно използване на устройства | **Контрол:**<br>Всички елементи на устройство, съдържащо запаметяващи носители, трябва да бъдат проверявани, за да се гарантира, че всякакви чувствителни данни и лицензиран софтуер са премахнати или сигурно презаписани преди унищожаването или повторното използване. | Да<br>√ | Не | |
| A.11.2.8 | **Дейност:**<br>Ненадзиравани потребителски устройства | **Контрол:**<br>Потребителите трябва да осигурят оставените без надзор устройства да са подходящо защитени. | Да<br>√ | Не | |
| A.11.2.9 | **Дейност:**<br>Политика за чисто бюро и чист екран | **Контрол:**<br>Трябва да бъде приета политика за бюро, чисто от хартиени документи и преносими информационни носители, и политика за чист екран при средствата за обработване на информация. | Да<br>√ | Не | |
| **A.12** | **Сигурност на работата** | | | | |
| **A.12.1** | **Процедури за работа и отговорности** | | | | |
| ***Цел:*** *Да се осигури правилна и сигурна работа на средствата за обработване на информация.* | | | | | |
| A.12.1.1 | **Дейност:**<br>Документирани процедури за работа | **Контрол:**<br>Процедурите за работа трябва да бъдат документирани и достъпни за всички потребители, които се нуждаят от тях. | Да<br>√ | Не | |
| A.12.1.2 | **Дейност:**<br>Управление на измененията | **Контрол:**<br>Измененията в организацията, процесите на дейността и средствата и системите за обработване на информация трябва да бъдат контролирани. | Да<br>√ | Не | |
| A.12.1.3 | **Дейност:**<br>Управление на капацитета | **Контрол:**<br>Използването на ресурсите трябва да бъде наблюдавано, регулирано и да се предвиждат бъдещи изисквания за капацитета, за да се гарантира изискваната производителност на системата. | Да<br>√ | Не | |

| | | | | | |
|---|---|---|---|---|---|
| A.12.1.4 | **Дейност:**<br>Отделяне на средите за разработване, изпитване и работа | **Контрол:**<br>Средите за разработване, изпитване и работа трябва да бъдат отделени, за да се намалят рисковете от неоторизиран достъп или изменения в средата на работа. | Да<br>√ | Не | |
| **A.12.2** | **Защита от злонамерен софтуер** | | | | |
| ***Цел:*** *Да се осигури защитата на информацията и средствата за обработване на информация от злонамерен софтуер.* | | | | | |
| A.12.2.1 | **Дейност:**<br>Механизми за контрол срещу злонамерен софтуер | **Контрол:**<br>Трябва да бъдат прилагани механизми за контрол за откриване, предотвратяване и възстановяване, които да защитят от злонамерен софтуер и които са съчетани с подходящо осведомяване на потребителите. | Да<br>√ | Не | |
| **A.12.3** | **Резервиране** | | | | |
| ***Цел:*** *Да защити от загуба на данни.* | | | | | |
| A.12.3.1 | **Дейност:**<br>Резервиране на информация | **Контрол:**<br>Трябва да бъдат направени и редовно изпитвани резервни копия на информация, софтуер и образи на системите в съответствие с договорената политика за резервиране. | Да<br>√ | Не | |
| **A.12.4** | **Регистриране и наблюдение** | | | | |
| ***Цел:*** *Да се записват събития и да се създадат доказателства.* | | | | | |
| A.12.4.1 | **Дейност:**<br>Регистриране на събития | **Контрол:**<br>Трябва да бъдат изработвани, съхранявани и редовно извършвани прегледи на регистри за събития, записващи дейности на потребители, изключителни случаи, грешки и събития, свързани със сигурността на информацията. | Да<br>√ | Не | |
| A.12.4.2 | **Дейност:**<br>Защита на регистрираната информация | **Контрол:**<br>Средствата за регистрация и регистрираната информация трябва да бъдат защитени от подправяне и неоторизиран достъп. | Да<br>√ | Не | |
| A.12.4.3 | **Дейност:**<br>Дневници на действията на системния администратор и оператора | **Контрол:**<br>Действията на системния администратор и оператора трябва да бъдат регистрирани, като дневниците трябва да бъдат защитени и редовно преглеждани. | Да<br>√ | Не | |
| A.12.4.4 | **Дейност:**<br>Синхронизация на часовниците | **Контрол:**<br>Часовниците на всички системи за обработване на информация в организацията или зоната за сигурност трябва да бъдат синхронизирани с един единствен опорен източник на точно време. | Да<br>√ | Не | |
| **A.12.5** | **Контрол на работещия софтуер** | | | | |
| ***Цел:*** *Да се осигури цялостността на работещите системи.* | | | | | |
| A.12.5.1 | **Дейност:**<br>Инсталиране на софтуер върху работещи системи | **Контрол:**<br>Трябва да има внедрени процедури, контролиращи инсталирането на софтуер върху работещи системи. | Да<br>√ | Не | |

| | | | | | |
|---|---|---|---|---|---|
| **A.12.6** | **Управление на техническата уязвимост** | | | | |
| ***Цел:*** *Да се предотврати използването на технически уязвимости.* | | | | | |
| A.12.6.1 | **Дейност:**<br>Управление на техническите уязвимости | **Контрол:**<br>Трябва да бъде получена навременна информация за техническа уязвимост на използваните информационни системи; излагането на организацията на такава уязвимост трябва да бъде оценено и трябва да бъдат предприети мерки, за да се отговори на свързания с това риск. | Да<br>√ | Не | |
| A.12.6.2 | **Дейност:**<br>Ограничения при инсталиране на софтуер | **Контрол:**<br>Трябва да бъдат създадени и приложени правила, определящи инсталирането на софтуер от потребители. | Да<br>√ | Не | |
| **A. 12.7** | **Разглеждане на одита на информационни системи** | | | | |
| ***Цел:*** *Минимизиране на въздействието на процеса на одит върху работещите системи.* | | | | | |
| A.12.7.1 | **Дейност:**<br>Механизми за контрол при одит на информационни системи | **Контрол:**<br>Изискванията за одит и действията, включващи проверки на работещи системи, трябва да бъдат внимателно планирани и съгласувани, за да се минимизират нарушенията на процесите на дейността. | Да<br>√ | Не | |
| **A. 13** | **Сигурност на комуникациите** | | | | |
| **A. 13.1** | **Управление на сигурността на мрежите** | | | | |
| ***Цел:*** *Да се осигури защита на информацията в мрежите и поддържащите ги средства за обработване на информация.* | | | | | |
| A.13.1.1 | **Дейност:**<br>Механизми за контрол на мрежите | **Контрол:**<br>Мрежите трябва да бъдат управлявани и контролирани, за да защитят информацията в системите и приложенията. | Да<br>√ | Не | |
| A.13.1.2 | **Дейност:**<br>Сигурност на мрежови услуги | **Контрол:**<br>Механизмите за сигурност, нивата на услугата и изискванията за управление на всички мрежови услуги трябва да бъдат определени и включени във всяко споразумение за мрежови услуги, независимо от това, дали тези услуги се предоставят от самата организация или от външна организация. | Да<br>√ | Не | |
| A.13.1.3 | **Дейност:**<br>Разделяне в мрежите | **Контрол:**<br>Вътре в мрежите групите информационни услуги, потребители и информационни системи трябва да бъдат разделени. | Да<br>√ | Не | |
| **A.13.2** | **Обмен на информация** | | | | |
| ***Цел:*** *Да се поддържа сигурността на информацията, обменяна вътре в организацията или с външни страни.* | | | | | |
| A.13.2.1 | **Дейност:**<br>Политики и процедури за обмен на информация | **Контрол:**<br>Трябва да съществуват официални политики, процедури и механизми за контрол, за да се защити обменът на информация чрез използване на всички средства за комуникация. | Да<br>√ | Не | |
| A.13.2.2 | **Дейност:**<br>Споразумения за обмен на информация | **Контрол:**<br>При прехвърляне на информация за дейността между организацията и външни страни трябва да бъдат сключвани споразумения. | Да<br>√ | Не | |

| | | | | | |
|---|---|---|---|---|---|
| A.13.2.3 | **Дейност:**<br>Електронен обмен на съобщения | **Контрол:**<br>Информацията, съдържаща се в електронните съобщения, трябва да бъде подходящо защитена. | Да<br>√ | Не | |
| A.13.2.4 | **Дейност:**<br>Споразумения за поверителност или неразкриване на тайна | **Контрол:**<br>Трябва да бъдат определени, редовно преглеждани и документирани изисквания за споразумения за поверителност или за неразкриване на тайна, отразяващи потребностите на организацията от защита на информацията. | Да<br>√ | Не | |
| **A.14** | **Придобиване, разработване и поддържане на системи** | | | | |
| **A.14.1** | **Изисквания за сигурност на информационните системи** | | | | |
| ***Цел:*** *Да се гарантира, че сигурността на информацията е неразделна част от информационните системи през целия им жизнен цикъл. Това включва също изисквания към информационни системи, които предоставят услуги през обществени мрежи.* | | | | | |
| A.14.1.1 | **Дейност:**<br>Анализ и спецификация на изискванията за сигурност на информацията | **Контрол:**<br>Изискванията, имащи отношение към сигурността на информацията, трябва да бъдат включени в изискванията за нови информационни системи или подобряване на съществуващи информационни системи. | Да<br>√ | Не | |
| A.14.1.2 | **Дейност:**<br>Осигуряване на приложни услуги през обществени мрежи | **Контрол:**<br>Информацията, включена в приложни услуги, която преминава през обществени мрежи, трябва да бъде защитена от измамни действия, оспорване на договорни задължения и неоторизирано разкриване и изменение. | Да<br>√ | Не | |
| A.14.1.3 | **Дейност:**<br>Защита на транзакции на приложни услуги | **Контрол:**<br>Информацията, включена в транзакции на приложни услуги, трябва да бъде защитена, за да се предотврати непълно предаване, погрешно маршрутизиране, неоторизирано изменение на съобщението, неоторизирано разкриване, неоторизирано дублиране на съобщение или атака чрез възпроизвеждане. | Да | Не<br>√ | |
| **A.14.2** | **Сигурност при процесите на разработване и поддържане** | | | | |
| ***Цел:*** *Да се осигури, че сигурността на информацията е проектирана и осъществена в рамките на цикъла на разработване на информационните системи.* | | | | | |
| A.14.2.1 | **Дейност:**<br>Политика за сигурно разработване | **Контрол:**<br>В рамките на организацията трябва да бъдат установени и приложени правила за разработване на софтуер и системи. | Да | Не<br>√ | |
| A.14.2.2 | **Дейност:**<br>Процедури за контрол на измененията в системите | **Контрол:**<br>Извършването на изменения в системите в рамките на цикъла на разработване трябва да бъде контролирано чрез използване на официални процедури за контрол на измененията. | Да | Не<br>√ | |
| A.14.2.3 | **Дейност:**<br>Технически преглед на приложенията след изменения в оперативната платформа | **Контрол:**<br>При изменения в оперативните платформи критичните приложения на дейностите трябва да бъдат преглеждани и изпитвани, за да се гарантира, че няма неблагоприятно въздействие върху работата или сигурността на организацията. | Да | Не<br>√ | |
| A.14.2.4 | **Дейност:**<br>Ограничения върху измененията на софтуерните пакети | **Контрол:**<br>Модификации в софтуерните пакети трябва да бъдат избягвани, ограничени до необходимата степен и всички изменения трябва да бъдат строго контролирани. | Да | Не<br>√ | |

| | | | | | |
|---|---|---|---|---|---|
| A.14.2.5 | **Дейност:**<br>Инженерни принципи за сигурни системи | **Контрол:**<br>Инженерни принципи за сигурни системи трябва да бъдат създадени, документирани, поддържани и приложени при всеки опит за реализиране на информационна система. | Да | Не<br>√ | |
| A.14.2.6 | **Дейност:**<br>Сигурна среда за разработване | **Контрол:**<br>Организациите трябва да създадат и защитят по подходящ начин сигурна среда за разработване на опитите за разработване и интегриране на системи, която да обхваща целия цикъл на разработките. | Да | Не<br>√ | |
| A.14.2.7 | **Дейност:**<br>Разработване на софтуер от външни страни | **Контрол:**<br>Разработването на софтуер от външни страни трябва да бъде следено и наблюдавано от организацията. | Да | Не<br>√ | |
| A.14.2.8 | **Дейност:**<br>Изпитване на сигурността на системата | **Контрол:**<br>По време на разработването трябва да бъдат изпитани функционалните възможности по отношение на сигурността. | Да | Не<br>√ | |
| A.14.2.9 | **Дейност:**<br>Приемни изпитвания на системата | **Контрол:**<br>За нови информационни системи, подобрения и нови версии трябва да бъдат създадени програми за приемно изпитване и свързани с тях критерии. | Да | Не<br>√ | |
| **A.14.3** | **Данни при изпитване** | | | | |
| ***Цел:*** *Да се осигури защита на данните, използвани при изпитване.* | | | | | |
| A.14.3.1 | **Дейност:**<br>Защита на данните при изпитване | **Контрол:**<br>Данните за изпитването трябва да бъдат внимателно подбрани, защитени и контролирани. | Да | Не<br>√ | |
| **A.15** | **Взаимоотношения с доставчици** | | | | |
| **A.15.1** | **Сигурност на информацията при взаимоотношения с доставчици** | | | | |
| ***Цел:*** *Да се осигури защита на активите на организацията, които са достъпни за доставчика.* | | | | | |
| A.15.1.1 | **Дейност:**<br>Политика за сигурността на информацията при взаимоотношения с доставчици | **Контрол:**<br>С доставчика трябва да бъдат договорени и документирани изисквания за сигурност на информацията, които намаляват рисковете, свързани с достъпа на доставчика до активите на организацията. | Да<br>√ | Не | |
| A.15.1.2 | **Дейност:**<br>Разглеждане на сигурността в рамките на споразумения с доставчици | **Контрол:**<br>Всички приложими изисквания към сигурността на информацията трябва да бъдат въведени и съгласувани с всеки доставчик, който може да има достъп, да обработва, да съхранява, да разпространява или да предоставя ИТ инфраструктурни компоненти за информацията на организацията. | Да<br>√ | Не | |
| A.15.1.3 | **Дейност:**<br>Верига за доставки за информационни и комуникационни | **Контрол:**<br>Споразуменията с доставчиците трябва да включват изисквания,ъ2 отнасящи се за рисковете за сигурността на информацията, свързани с веригата за доставки на услуги и продукти на информационни и комуникационни технологии. | Да<br>√ | Не | |

| | | | | | |
|---|---|---|---|---|---|
| **A.15.2** | **Управление на предоставянето на услуги от доставчици** | | | | |
| ***Цел:*** *Да се поддържа договореното ниво на сигурност на информацията и предоставянето на услуги в съответствие със споразуменията с доставчици.* | | | | | |
| A.15.2.1 | **Дейност:**<br>Наблюдение и преглед на услуги, предоставяни от доставчици | **Контрол:**<br>Организациите трябва редовно да наблюдават, преглеждат и одитират предоставянето на услуги от доставчиците. | Да<br>√ | Не | |
| A.15.2.2 | **Дейност:**<br>Управление на измененията на услугите, предоставяни от доставчици | **Контрол:**<br>Измененията на предоставянето на услуги от доставчици, съдържащи поддържане и усъвършенстване на съществуващи политики, процедури и механизми за контрол за сигурност на информацията, трябва да бъдат управлявани, като се отчита критичността на информацията, системите и процесите, свързани с дейността и повторно оценяване на рисковете. | Да<br>√ | Не | |
| **A.16** | **Управление на инциденти със сигурността на информацията** | | | | |
| **A.16.1** | **Управление на инциденти и подобряване на сигурността на информацията** | | | | |
| ***Цел:*** *Да се осигури последователен и ефикасен подход към управление на инцидентите със сигурността на информацията, включително съобщаване за събития и слабости, свързани със сигурността.* | | | | | |
| A.16.1.1 | **Дейност:**<br>Отговорности и процедури | **Контрол:**<br>Трябва да бъдат установени отговорности и процедури за управление, за да се осигури бърза, ефикасна и системна реакция на инцидентите със сигурността на информацията. | Да<br>√ | Не | |
| A.16.1.2 | **Дейност:**<br>Докладване за събития, свързани със сигурността на информацията | **Контрол:**<br>Събитията, свързани със сигурността на информацията, трябва да бъдат докладвани по съответни управленски канали възможно най- бързо. | Да<br>√ | Не | |
| A.16.1.3 | **Дейност:**<br>Докладване за слабости в сигурността на информацията | **Контрол:**<br>Трябва да се изисква от служителите и доставчиците, използващи информационните системи и услуги на организацията, да отбелязват и докладват всяка наблюдавана или предполагаема слабост в сигурността в системите или услугите. | Да<br>√ | Не | |
| A.16.1.4 | **Дейност:**<br>Оценяване на събития, свързани със сигурността на информацията, и вземане на решения за тях | **Контрол:**<br>Събитията, свързани със сигурността на информацията, трябва да бъдат оценени, като трябва да бъде решено дали те трябва да бъдат класифицирани като инциденти със сигурността. | Да<br>√ | Не | |
| A.16.1.5 | **Дейност:**<br>Реакция на инциденти със сигурността на информацията | **Контрол:**<br>На инцидентите със сигурността на информацията трябва да се реагира в съответствие с документирани процедури. | Да<br>√ | Не | |

| | | | | | |
|---|---|---|---|---|---|
| A.16.1.6 | **Дейност:**<br>Изводи от инцидентите със сигурността на информацията | **Контрол:**<br>Познанията, придобити при анализирането и разрешаването на инциденти със сигурността на информацията, трябва да бъдат използвани за намаляване на вероятността или въздействието на бъдещи инциденти. | Да<br>√ | Не | |
| A.16.1.7 | **Дейност:**<br>Събиране на доказателства | **Контрол:**<br>Организацията трябва да определи и прилага процедури за идентифициране, събиране, придобиване и съхраняване на информация, която може да послужи като доказателство. | Да<br>√ | Не | |
| **A.17** | **Аспекти на сигурността на информацията при управление на непрекъснатостта на дейността** | | | | |
| **A.17.1** | **Непрекъснатост на сигурността на информацията** | | | | |
| ***Цел:*** *Непрекъснатостта на сигурността на информацията трябва да бъде заложена в системите за управление на непрекъснатостта на дейността на организацията.* | | | | | |
| A.17.1.1 | **Дейност:**<br>Планиране на непрекъснатост на сигурността на информацията | **Контрол:**<br>Организацията трябва да определи своите изисквания за сигурност на информацията и за непрекъснатост на управлението на сигурността на информацията в неблагоприятни случаи, например по време на криза или бедствие. | Да<br>√ | Не | |
| A.17.1.2 | **Дейност:**<br>Осъществяване на непрекъснатост на сигурността на информацията | **Контрол:**<br>Организацията трябва да създаде, документира, осъществи и поддържа процеси, процедури и механизми за контрол, за да осигури необходимото ниво на непрекъснатост за сигурността на информацията по време на неблагоприятни случаи. | Да<br>√ | Не | |
| A.17.1.3 | **Дейност:**<br>Проверка, преглед и оценяване на непрекъснатостта на сигурността на информацията | **Контрол:**<br>Организацията трябва да проверява през редовни интервали създадените и осъществени механизми за контрол на непрекъснатостта на сигурността на информацията, така че да осигури, че те са действащи и ефикасни по време на неблагоприятни случаи. | Да<br>√ | Не | |
| **A.17.2** | **Излишък** | | | | |
| ***Цел:*** *Да се осигури готовност на средствата за обработване на информация.* | | | | | |
| A.17.2.1 | **Дейност:**<br>Готовност на средствата за обработване на информация | **Контрол:**<br>Средствата за обработване на информация трябва да бъдат осъществени с излишък, достатъчен за отговаряне на изискванията за готовност. | Да<br>√ | Не | |
| **A.18** | **Съответствие** | | | | |
| **A.18.1** | **Съответствие със законови и договорни изисквания** | | | | |
| ***Цел:*** *Да се избегнат нарушения на правни, законови, нормативни или договорни задължения, отнасящи се за сигурността на информацията, както и на всички изисквания за сигурност.* | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| A.18.1.1 | **Дейност:**<br>Идентифициране на приложимите законови и договорни изисквания | **Контрол:**<br>Всички съответни правни, законови, нормативни и договорни изисквания и подходът на организацията за удовлетворяване на тези изисквания трябва да бъдат изрично идентифицирани, документирани и актуализирани за всяка информационна система и за организацията. | Да<br>√ | Не | |
| A.18.1.2 | **Дейност:**<br>Права на интелектуална собственост | **Контрол:**<br>Трябва да бъдат изпълнени съответни процедури, за да се осигури съответствие със законовите, нормативните и договорните изисквания по отношение на правата на интелектуална собственост и използване на патентовани софтуерни продукти. | Да<br>√ | Не | |
| A.18.1.3 | **Дейност:**<br>Защита на записите | **Контрол:**<br>Записите трябва да бъдат защитени от изгубване, разрушаване, фалшифициране, неоторизиран достъп или неоторизирано огласяване в съответствие със законовите, нормативните и договорните изисквания и изискванията за дейността. | Да<br>√ | Не | |
| A.18.1.4 | **Дейност:**<br>Тайна и защита на информацията за самоличността | **Контрол:**<br>Трябва да бъде осигурена тайната и защитата на информацията за самоличността според изискванията на съответните нормативни актове и регламенти, където са приложими. | Да<br>√ | Не | |
| A.18.1.5 | **Дейност:**<br>Регламентиране на криптографските механизми за контрол | **Контрол:**<br>Криптографските механизми за контрол трябва да се използват в съответствие с всички приложими споразумения, нормативни актове и регламенти. | Да<br>√ | Не | |
| **A.18.2** | **Прегледи на сигурността на информацията** | | | | |
| ***Цел:*** *Да се осигури, че сигурността на информацията е осъществена и функционира в съответствие с политиките и процедурите на организацията.* | | | | | |
| A.18.2.1 | **Дейност:**<br>Независим преглед на сигурността на информацията | **Контрол:**<br>През планирани интервали или при настъпили съществени промени трябва да се извършва независим преглед на подхода на организацията за управление на сигурността на информацията и неговото прилагане (т.е. целите на контрола, механизмите за контрол, политиките, процесите и процедурите за сигурност на информацията). | Да<br>√ | Не | - |
| A.18.2.2 | **Дейност:**<br>Съответствие с политиката и стандартите за сигурност | **Контрол:**<br>Ръководителите трябва редовно да преглеждат доколко обработването на информация и процедурите в тяхната област на отговорност съответстват на подходящите политики за сигурност, стандарти и всякакви други изисквания за сигурност. | Да<br>√ | Не | |
| A.18.2.3 | **Дейност:**<br>Преглед на техническото съответствие | **Контрол:**<br>Информационните системи трябва редовно да се преглеждат за съответствие с политиките за сигурност на информацията в организацията и стандартите. | Да<br>√ | Не | |

**Забележка:** *Посочените в Italic и Bold са планирани контроли от плана за третиране на риска.*

**ЗАКЛЮЧЕНИЕ:**

*Като обобщение, бих искал да подчертая, че за да се гарантира сигурност на информацията системата за управление на нейната защита трябва да обхваща цялата организация. Защитата на информацията се осигурява от всички хора в нея, а не само от различни технологии и мерки. Всички контролни дейности в една СУИС трябва да се избират на базата на оценка на риска. Системата трябва да е ресурсно осигурена и мениджмънта на организацията трябва да е ангажиран с въпросите за сигурността на информацията. Постигането на целта на системата за управление на информационната сигурност може да се осигури само ако цялата система работи, непрекъснато се контролира, оценява и постоянно се усъвършенства.*

**РАЗРАБОТИЛ,**
**ПРЕДСТАВИТЕЛ НА РЪКОВОДСТВОТО:**
**/Момчил Николов/**

| |
|---|
| *Идентификация на статуса: ОД 09_02-04 Версия 03/20.05.2015 г.* |
| *Ниво на достъп:* ■ *общодостъпен* ☐ *служебна информация* |
| [1]*Система за управление на информационната сигурност - server* |

[1] Попълва се само за документи, чиито форми се попълват или поддържат в електронен вид